

Classification of Maximal Arcs in Small Projective Hjelmslev Geometries

Thomas Honold and Michael Kiermaier

ABSTRACT. Maximal arcs in small projective Hjelmslev geometries are classified up to isomorphism, and the parameters of the associated codes are determined.

1. Introduction

Fat¹ linear codes over a finite chain ring R may be viewed as multisets of points in projective Hjelmslev geometries over R as developed in [6]. There is evidence that, just as in the classical case $R = \mathbb{F}_q$, good (from a coding theorist's point-of-view) linear codes over R correspond in general to interesting (from a geometer's point-of-view) multisets of points in projective Hjelmslev geometries.

This paper reports on a computer search for maximal arcs in projective Hjelmslev geometries of small dimension over chain rings of order at most 16. In the cases under consideration the arcs have been classified up to geometric equivalence.

We refer to [2, 7, 8, 10] for the combinatorics of projective Hjelmslev geometries and in particular for results on arcs in projective Hjelmslev planes. Some general properties of the MDS-like codes associated with arcs can be found in [5].

With a finite chain ring R (*not* assumed to be commutative) we associate the pair of parameters (q, m) , where $R/\text{rad } R \cong \mathbb{F}_q = \mathbb{F}_{p^r}$ and m is the composition length of ${}_R R$ (or R_R). Then R has cardinality q^m and characteristic p^λ , where $1 \leq \lambda \leq m$. Up to isomorphism there is only one ring with $\lambda = m$, the Galois ring $\mathbb{G}_{q,m} = \text{GR}(q^m, p^m)$, and one commutative ring with $\lambda = 1$, the truncated polynomial ring $\mathbb{S}_{q,m} = \mathbb{F}_q[X]/(X^m)$. The remaining chain rings of order ≤ 16 are $\mathbb{H}_8 = \mathbb{Z}_4[X]/(X^2 + 2, X^3)$, the truncated skew polynomial ring $\mathbb{T}_4 = \mathbb{F}_4[X; \sigma]/(X^2)$ w.r.t. $\sigma: \mathbb{F}_4 \rightarrow \mathbb{F}_4, a \mapsto a^2$, and the rings $\mathbb{I}_{16} = \mathbb{Z}_4[X]/(X^2 + 2)$, $\mathbb{J}_{16} = \mathbb{Z}_4[X]/(X^2 + 2X + 2)$, $\mathbb{K}_{16} = \mathbb{Z}_4[X]/(X^3 + 2, X^4)$. These rings have orders as indicated by the subscript.²

Denoting by R one of the rings listed above, we write $\text{PHG}(k, R)$ for the k -dimensional projective Hjelmslev geometry over R .³ The points (lines, hyperplanes) of $\text{PHG}(k, R)$ are the free rank 1 (rank 2, resp. rank k) submodules of a free R -module of rank $k + 1$, say R_R^{k+1} , and incidence is defined by set inclusion.

Key words and phrases. Codes over chain rings, projective Hjelmslev geometry, maximal arc, nauty.

¹A linear code is *fat* if its coordinate projections are onto.

²No rule without exception. The second author denies any responsibility for the weird ' \mathbb{T}_4 '.

³Even in the case of \mathbb{T}_4 there is no need to distinguish between “left” and “right” geometries. The antiautomorphism $a_0 + a_1X \mapsto a_0 + \sigma(a_1)X$ of \mathbb{T}_4 identifies $\text{PHG}(\mathbb{T}_4(\mathbb{T}_4^l))$ with $\text{PHG}((\mathbb{T}_4^l)_{\mathbb{T}_4})$.

(q, m)		$(2, 2)$		$(2, 3)$			$(3, 2)$		$(4, 2)$			$(2, 4)$				
k	u	\mathbb{Z}_4	$\mathbb{S}_{2,2}$	\mathbb{Z}_8	\mathbb{H}_8	$\mathbb{S}_{2,3}$	\mathbb{Z}_9	$\mathbb{S}_{3,2}$	$\mathbb{G}_{4,2}$	$\mathbb{S}_{4,2}$	\mathbb{T}_4	\mathbb{Z}_{16}	\mathbb{I}_{16}	\mathbb{J}_{16}	\mathbb{K}_{16}	$\mathbb{S}_{2,4}$
2	2	7	6_2	10	10_5	10_5	9_3	9_4	21	18_6	18	≥ 16				
	3	10_8	10_8	21	18_{93}	18_{93}	19_3	18_{255}								
	4	16_3	16_3													
	5	22	22													
	6	28	28													
3	3	8	$6_{1(2)}$	$8_{57(68)}$	9	9	10	10								
	4	10_{25}	11													
	5	16_2	16_2													
4	4	$6_{5(17)}$	$6_{5(17)}$													
	5	11_4	11_6													

TABLE 1. Cardinalities and number of equivalence classes of maximal (n, u) -arcs in $\text{PHG}(k, R)$, $|R| \leq 16$

Following the notation in [4, Ch. 3.3], an (n, u) -arc in $\text{PHG}(k, R)$ is an n -multiset of points of $\text{PHG}(k, R)$ with at most u points (counted with their multiplicities) on any hyperplane. An (n, u) -arc is called *degenerate* if its points (i. e. those of nonzero multiplicity) generate a proper submodule of R_R^{k+1} . We denote by $m_u(k, R)$ the maximum n for which an (n, u) -arc in $\text{PHG}(k, R)$ exists. An (n, u) -arc is said to be *complete* if it is not contained in an $(n+1, u)$ -arc and *maximal* if $n = m_u(k, R)$.

An n -multiset \mathfrak{k} of points of $\text{PHG}(k, R)$ defines an R -linear code $C \leq_R R^n$ by taking representative vectors of the points as columns of a generator matrix for C . Using a generalized Gray map $\psi: R \rightarrow \mathbb{F}_q^{q^{m-1}}$ as in [3], we obtain from C a (not necessarily linear) distance-invariant q -ary code $\psi(C)$.⁴ The weight distribution of $\psi(C)$ can be computed from geometric information on \mathfrak{k} ; see [6, Th. 5.2].

2. The Arcs

In [12] G.F. Royle describes an algorithm for the classification of complete arcs in projective planes over finite fields. The algorithm essentially applies B.D. McKay's isomorph-free exhaustive generation method for combinatorial structures (cf. [11] and the software package *nauty* available at <http://cs.anu.edu.au/~bdm/nauty/>) to the point-line incidence graph of the plane.

The second author [9] has adapted Royle's algorithm to the case $\text{PHG}(k, R)$. In particular, the classification of complete arcs in $\text{PHG}(k, R)$ is accomplished by applying the method to the point-hyperplane incidence graph of $\text{PHG}(k, R)$.

Table 1 shows the main results of this computer search. Tabulated are the numbers $m_u(k, R)$ for the chain rings of order ≤ 16 and small k, u , along with the number of equivalence classes of (n, u) -arcs, $n = m_u(k, R)$. Unique (up to equivalence) maximal arcs are indicated by bold type, otherwise the number of equivalence classes of nondegenerate maximal arcs (the total number of equivalence classes of maximal arcs) is appended as a subscript (resp. a subscript in parentheses).

Selected maximal arcs from Table 1 are listed in the appendix, along with data on the Gray images of the associated R -linear codes.

⁴If R has prime characteristic p then $\psi(C)$ is in fact a linear code.

3. Remarks

For chain rings of length $m = 2$, the numbers $m_u(2, R)$ were known previously except for the cases $m_2(2, \mathbb{S}_{2,2}) = m_2(2, \mathbb{T}_4) = 18$; cf. [2, 7, 8, 10].

It has been conjectured before that for given q, m, k, u , the numbers $m_u(k, R)$ form a non-decreasing function of the characteristic of R . This is not true in general, as the example of the (unique) $(11, 4)$ -arc in $\text{PHG}(3, \mathbb{S}_{2,2})$ shows which is bigger than any $(n, 4)$ -arc in $\text{PHG}(3, \mathbb{Z}_4)$.

A $(q^m + q^{m-1} + 1, 2)$ -arc in $\text{PHG}(2, R)$ is also referred to as a *hyperoval*. Through any point of $\text{PHG}(2, R)$ there are $q^m + q^{m-1}$ lines, so hyperovals have no tangents. It is known that hyperovals in $\text{PHG}(2, R)$ exist iff $R = \mathbb{F}_{2^r}$ (a finite field of even order) or $R = \mathbb{G}_{2^r, 2}$ (a Galois ring of characteristic 4): The case $m = 1$ is classical, $m = 2$ has been done in [8], and for $m \geq 3$ the nonexistence of hyperovals in $\text{PHG}(2, R)$ follows from the observation that any two points of a hyperoval are on a unique secant (so the number of points cannot exceed $q^2 + q + 1$).

According to Table 1 hyperovals in the planes over \mathbb{Z}_4 and $\mathbb{G}_{4,2}$ are unique up to equivalence. The following proposition gives a bit more information on hyperovals in $\text{PHG}(\mathbb{Z}_4)$.

PROPOSITION. *The set \mathfrak{H} of hyperovals of $\text{PHG}(2, \mathbb{Z}_4)$ has cardinality 256. The automorphism group G of $\text{PHG}(2, \mathbb{Z}_4)$ is transitive on \mathfrak{H} and the stabilizer $G_{\mathfrak{h}}$ of a hyperoval $\mathfrak{h} \in \mathfrak{H}$ has order 168. Further, G has a normal subgroup H which is regular on \mathfrak{H} .*

PROOF. The group $\text{PGL}(3, \mathbb{Z}_4)$ acts regularly on ordered quadrangles (four points in different neighbour classes, no three neighbour classes on a line of the quotient plane $\text{PG}(2, \mathbb{F}_2)$). The stabilizer in G of an ordered quadrangle is easily seen to be trivial. Hence $G \cong \text{PGL}(3, \mathbb{Z}_4)$ (an instance of the Fundamental Theorem of Projective Hjelmslev Geometry) and $|G| = |\text{PGL}(3, \mathbb{Z}_4)| = 2^9 \cdot |\text{GL}(3, 2)|/2 = 256 \cdot 168$. Now observe that a quadrangle is contained in a unique hyperoval—for the canonical quadrangle $\mathbb{Z}_4(100)$, $\mathbb{Z}_4(010)$, $\mathbb{Z}_4(001)$, $\mathbb{Z}_4(111)$ the remaining points are $\mathbb{Z}_4(123)$, $\mathbb{Z}_4(312)$ and $\mathbb{Z}_4(231)$ —and a hyperoval contains 168 ordered quadrangles—as many as the quotient plane $\text{PG}(2, \mathbb{F}_2)$. This yields all except the last assertion. Finally, since each $G_{\mathfrak{h}} \cong \text{GL}(3, 2)$ acts faithfully on the quotient plane, the required normal subgroup of G is the kernel of the action of G on the quotient plane, i. e. $H = (\mathbf{I}_3 + 2\mathbb{Z}_4^{3 \times 3})/\{\pm \mathbf{I}_3\}$, where \mathbf{I}_3 denotes the 3×3 identity matrix. \square

We leave it as an exercise to prove the uniqueness of the $(8, 3)$ -arc of $\text{PHG}(3, \mathbb{Z}_4)$ (which corresponds to the \mathbb{Z}_4 -linear Nordstrom-Robinson code) along similar lines.

Appendix

Data on selected arcs from Table 1 is given below. Each entry contains the arc (in homogeneous coordinates), the order g of its automorphism group, the minimum homogeneous distance d_{hom} of the associated code C (which is equal to q^{2-m} times the minimum Hamming distance of the Gray image) and information on the q -ary Gray image $\psi(C)$.

(7, 2)-arc in $\text{PHG}(2, \mathbb{Z}_4)$:

$(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1), (2 : 1 : 3), (1 : 2 : 3), (1 : 3 : 2)$

$g = 168, d_{\text{hom}} = 6$

ψ gives a binary $[14, 6, 6]$ -code with weight enumerator $1 + 42X^6 + 7X^8 + 14X^{10}$.

The best linear binary $[14, 6]$ -code has minimum distance 5.

(22, 5)-arc in PHG(2, \mathbb{Z}_4):

$$g = 1536, d_{\text{hom}} = 20$$

$(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1), (0 : 1 : 1), (1 : 0 : 1), (1 : 1 : 0),$
 $(1 : 2 : 2), (2 : 1 : 2), (2 : 2 : 1), (1 : 3 : 3), (2 : 1 : 3), (1 : 2 : 3), (1 : 3 : 2),$
 $(1 : 2 : 0), (2 : 1 : 0), (2 : 0 : 1), (1 : 3 : 1), (1 : 0 : 2), (0 : 1 : 2), (0 : 2 : 1),$
 $(1 : 1 : 3)$

ψ gives a binary $[44, 6, 20]$ -code with weight enumerator $1 + 6X^{20} + 48X^{22} + 6X^{24} + 2X^{28} + X^{32}$. There is a linear binary $[44, 6, 21]$ -code.

(22, 5)-arc in PHG(2, $\mathbb{S}_{2,2}$):

$$g = 1536, d_{\text{hom}} = 20$$

$(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1), (0 : 1 : 1), (1 : 0 : 1), (1 : X : X),$
 $(X : 1 : X), (X : X : 1), (1 : X + 1 : X + 1), (X : 1 : X + 1), (1 : X : X + 1),$
 $(1 : X : 0), (X : 1 : 0), (X : 0 : 1), (1 : X + 1 : 1), (1 : X + 1 : 0),$
 $(1 : 0 : X), (0 : 1 : X), (0 : X : 1), (1 : 1 : X + 1), (1 : 1 : X)$

ψ gives a linear binary code with the same parameters as in the last case.

(8, 3)-arc in PHG(3, \mathbb{Z}_4):

$$g = 1344, d_{\text{hom}} = 6$$

$(1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0), (0 : 0 : 0 : 1), (1 : 3 : 3 : 2),$
 $(2 : 1 : 3 : 3), (1 : 2 : 1 : 3), (1 : 1 : 2 : 1)$

ψ gives a binary $[16, 8, 6]$ -code with weight enumerator $1 + 112X^6 + 30X^8 + 112X^{10} + X^{16}$. The best linear binary $[16, 8]$ -code has minimum distance 5.

(11, 4)-arc in PHG(3, $\mathbb{S}_{2,2}$):

$$g = 24, d_{\text{hom}} = 8$$

$(1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0), (0 : 0 : 0 : 1), (1 : 1 : 1 : 1),$
 $(X : 1 : X + 1 : X), (1 : X : X + 1 : X + 1), (1 : X : 1 : X),$
 $(1 : X + 1 : 0 : X), (1 : X + 1 : X + 1 : 0), (0 : 1 : X : X + 1)$

ψ gives a linear binary $[22, 8, 8]$ -code with weight enumerator $1 + 54X^8 + 76X^{10} + 72X^{12} + 48X^{14} + X^{16} + 4X^{18}$ which is optimal.

(10, 2)-arc in PHG(2, \mathbb{Z}_8):

$$g = 8, d_{\text{hom}} = 6$$

$(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1), (2 : 1 : 3), (4 : 1 : 5), (1 : 5 : 4),$
 $(6 : 1 : 2), (1 : 7 : 2), (1 : 3 : 5)$

ψ gives a binary $[40, 9, 12]$ -code with weight enumerator $1 + 4X^{12} + 70X^{16} + 128X^{18} + 168X^{20} + 32X^{22} + 72X^{24} + 32X^{26} + 4X^{28} + X^{32}$. There is a linear binary $[40, 9, 16]$ -code.

(21, 3)-arc in PHG(2, \mathbb{Z}_8):

$$g = 168, d_{\text{hom}} = 18$$

$(1 : 0 : 0), (0 : 1 : 0), (1 : 2 : 2), (2 : 2 : 1), (2 : 1 : 3), (1 : 2 : 1), (1 : 1 : 3),$
 $(1 : 1 : 2), (1 : 5 : 5), (1 : 5 : 4), (1 : 7 : 6), (6 : 1 : 5), (4 : 1 : 7), (6 : 1 : 0),$
 $(1 : 7 : 1), (0 : 4 : 1), (1 : 0 : 5), (2 : 1 : 6), (1 : 2 : 7), (1 : 0 : 6), (0 : 6 : 1)$

ψ gives a binary $[84, 9, 36]$ -code with weight enumerator $1 + 14X^{36} + 168X^{38} + 196X^{42} + 42X^{44} + 7X^{48} + 84X^{50}$. There is a linear binary $[84, 9, 38]$ -code.

(9, 3)-arc in PHG(3, \mathbb{H}_8):

$$g = 12, d_{\text{hom}} = 5$$

$(1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0), (0 : 0 : 0 : 1), (1 : X : X + 1 : X),$
 $(X : X : 1 : X + 1), (1 : X + 3 : 2 : X + 2), (2 : 1 : X + 3 : X + 3),$
 $(1 : 2 : X + 3 : X + 1)$

ψ gives a binary $[36, 12, 10]$ -code with weight enumerator $1 + 12X^{10} + 166X^{12} + 504X^{14} + 873X^{16} + 908X^{18} + 1020X^{20} + 468X^{22} + 110X^{24} + 24X^{26} + 6X^{28} + 4X^{30}$.
There is a linear binary $[36, 12, 12]$ -code.

(9, 3)-arc in $\text{PHG}(3, \mathbb{S}_{2,3})$:

$g = 12, d_{\text{hom}} = 5$

$(1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0), (0 : 0 : 0 : 1), (1 : X : X + 1 : X),$
 $(X^2 + X : 1 : X^2 + X + 1 : X^2 + X), (1 : X^2 + X + 1 : X^2 : X^2 + X),$
 $(1 : X^2 : X^2 + X + 1 : X^2 + X + 1), (X^2 : 1 : X + 1 : X^2 + X + 1)$

ψ gives a linear binary code with the same parameters as in the last case.

(10, 3)-arc in $\text{PHG}(3, \mathbb{Z}_9)$:

$g = 10, d_{\text{hom}} = 15$

$(1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0), (0 : 0 : 0 : 1), (1 : 1 : 1 : 1),$
 $(1 : 3 : 2 : 4), (1 : 4 : 3 : 2), (1 : 2 : 8 : 3), (3 : 1 : 8 : 2), (1 : 8 : 4 : 5)$

ψ gives a ternary $[30, 8, 15]$ -code with weight enumerator $1 + 720X^{15} + 1680X^{18} + 3240X^{21} + 900X^{24} + 20X^{27}$. There no better linear ternary $[30, 8]$ -code.

(10, 3)-arc in $\text{PHG}(3, \mathbb{S}_{3,2})$:

$g = 10, d_{\text{hom}} = 15$

$(1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0), (0 : 0 : 0 : 1), (1 : 1 : 1 : 1),$
 $(1 : X : X + 2 : X + 1), (1 : X + 2 : 2 : 2X), (1 : 2X + 2 : 2X + 1 : X + 2),$
 $(1 : 2X + 1 : X : 2X + 2), (2X : 1 : X + 2 : 2X + 2)$

ψ gives an (optimal) linear ternary code with the same parameters as in the last case.

(21, 2)-arc in $\text{PHG}(2, \mathbb{G}_{4,2})$:

$g = 126, d_{\text{hom}} = 60$

$(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1), (1 : 3 : 3a), (2 : 1 : 3a), (1 : 3a : 2a + 2),$
 $(1 : a + 3 : 2a), (1 : 2 : a + 1), (1 : 2a + 3 : 2), (1 : 2a + 2 : 3), (2a + 2 : 1 : 3a + 3),$
 $(1 : a : 3a + 1), (1 : 3a + 3 : a + 2), (2a : 1 : 3), (1 : 2a + 1 : 3a + 3), (1 : a + 2 : a),$
 $(1 : 3a + 1 : 2a + 3), (1 : 2a : 3a + 2), (1 : a + 1 : a + 3), (1 : 3a + 2 : 2a + 1)$

ψ gives a quaternary $[84, 6, 60]$ -code with weight enumerator $1 + 2520X^{60} + 63X^{64} + 1512X^{68}$. The best known linear quaternary $[84, 6]$ -code has minimum distance 59.

(18, 2)-arc in $\text{PHG}(2, \mathbb{T}_4)$:

$g = 96, d_{\text{hom}} = 48$

$(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1), (1 : X + 1 : X + a), (1 : X + a : X),$
 $(1 : X : aX + 1), (1 : X + (a + 1) : a), (aX : 1 : X + 1), (1 : aX : aX + a),$
 $(1 : aX + a : (a + 1)X + a), (1 : aX + (a + 1) : (a + 1)X + 1),$
 $(1 : (a + 1)X + a : X + 1), (1 : (a + 1)X + 1 : aX + (a + 1)),$
 $(1 : (a + 1)X + (a + 1) : aX), ((a + 1)X : 1 : aX + a),$
 $(1 : a + 1 : X + (a + 1)), (1 : a : (a + 1)X + (a + 1))$

ψ gives a linear quaternary $[72, 6, 48]$ -code with weight enumerator $1 + 12X^{48} + 864X^{50} + 960X^{51} + 96X^{52} + 576X^{54} + 144X^{56} + 864X^{58} + 576X^{59} + 3X^{64}$. There is a linear quaternary $[72, 6, 50]$ -code.

References

- [1] *Proceedings of the Ninth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-2004)*, Kranevo, Bulgaria, 2004.

- [2] S. Boumova and I. Landjev. Some new arcs in projective Hjelmslev planes over chain rings. In ACCT9 [1], pages 56–61.
- [3] M. Greferath and S. E. Schmidt. Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *IEEE Transactions on Information Theory*, 45(7):2522–2524, Nov. 1999.
- [4] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford University Press, 2nd edition, 1998.
- [5] T. Honold. Arcs and MDS-like codes over finite chain rings. In ACCT9 [1], pages 223–229.
- [6] T. Honold and I. Landjev. Linear codes over finite chain rings. *Electronic Journal of Combinatorics*, 7:Research Paper 11, 22 pp. (electronic), 2000.
- [7] T. Honold and I. Landjev. On arcs in projective Hjelmslev planes. *Discrete Mathematics*, 231(1-3):265–278, 2001. 17th British Combinatorial Conference, University of Kent, Canterbury, 1999.
- [8] T. Honold and I. Landjev. On maximal arcs in projective Hjelmslev planes over chain rings of even characteristic. *Finite Fields and their Applications*, 11(2):292–304, 2005.
- [9] M. Kiermaier. Arcs und Codes über endlichen Kettenringen. Diplomarbeit, Technische Universität München, Apr. 2006.
- [10] I. Landjev and T. Honold. Arcs in projective Hjelmslev planes. *Discrete Mathematics and Applications*, 11(1):53–70, 2001. Originally published in *Diskretnaya Matematika* (2001) 13, No. 1, 90–109 (in Russian).
- [11] B. D. McKay. Isomorph-free exhaustive generation. *Journal of Algorithms*, 26:306–324, 1998.
- [12] G. F. Royle. An orderly algorithm and some applications in finite geometry. *Discrete Mathematics*, 185:105–115, 1998.

THOMAS HONOLD, TECHNISCHE UNIVERSITÄT MÜNCHEN, ZENTRUM MATHEMATIK (M11), BOLTZMANNSTR. 3, D-85748 GARCHING, GERMANY

E-mail address: honold@ma.tum.de

MICHAEL KIERMAIER, TECHNISCHE UNIVERSITÄT MÜNCHEN, ZENTRUM MATHEMATIK (M11), BOLTZMANNSTR. 3, D-85748 GARCHING, GERMANY

E-mail address: michael.kiermaier@gmx.net